ABSTRACT

A monitoring system monitors a system that has multiple devices that perform respective primary tasks. For the purpose of the monitoring, each device has a finite state machine (FSM) with stochastic non-periodic behavior. The monitoring system simulates in software the behavior of the FSM's. A discrepancy between the states assumed by the FSM's after each time step and the states assumed in the simulation in each time step indicates a failure or a breach of the network's integrity. Hacking such as primary system is practically impossible without being detected. Each device comprises computational resources. In order to reduce the computational environment available to a virus, the idle time of the resources is absorbed by dynamically increasing the complexity of the FSM's.